UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,917	06/26/2003	Kyung-Hun Jang	12000.SMG.0021	8113

48356 7590 12/18/2008

MCNEELY BODENDORF LLP
P.O. BOX 34175
WASHINGTON, DC 20043

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/607,917	JANG ET AL.	
	Examiner	Art Unit	
	BRANDON S. HOFFMAN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-8,10-12 and 14* is/are rejected.

7)☒ Claim(s) *2,9,13 and 15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending in this office action.

2. Applicant's arguments, filed September 19, 2008, have been fully considered and they are persuasive. However, a new ground of rejection is made.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claim 1, 3-8, and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eskicioglu (U.S. Patent Pub. No. 2002/0108040) in view of Watanabe et al. (U.S. Patent No. 7,072,657).

Regarding claims 1, 8, 11, and 12, Eskicioglu teaches a roaming method/computer readable storage medium/apparatus for a wireless station using a plurality of encryption keys differentiated according to a plurality of access authorization classes, the differentiated encryption keys provided to communicate data with corresponding access points, said method comprising the steps of:

- Obtaining by a wireless station in advance an encryption key set including the differentiated encryption keys for the corresponding access points when initial authentication of the wireless station is performed (paragraph 0038);
- Receiving a command to communicate with an access point not available for communication using an encryption key currently selected in the encryption key set (0047);
- Selecting an encryption key from the encryption key set obtained in advance corresponding to the determined access authorization (paragraph 0088-0092); and
- Using the selected encryption key to encrypt data and communicate with the access point not available for communication (paragraph 0094).

Eskicioglu does not teach determining an access authorization to the access point not available for communications.

Watanabe et al. teaches determining an access authorization to the access point not available for communications (col. 7, lines 4-6).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine determining an access authorization to the access point not available for communications, as taught by Watanabe et al., with the method

of Eskicioglu. It would have been obvious for such modifications because the proper access authorization ensures the proper credentials are given to gain access.

Regarding claim 3, Eskicioglu as modified by Watanabe et al. teaches further comprising: the wireless station desiring to communicate with an access point selecting from the differentiated encryption keys an encryption key corresponding to access authorization to the access point and communicates data with the access point (see col. 7, lines 17-40 of Watanabe et al.).

Regarding claims 4 and 10, Eskicioglu as modified by Watanabe et al. teaches wherein the obtaining of the differentiated encryption keys comprises:

- Determining access authorization to the access point when the access point is requested to perform initial authentication by the wireless station (see fig. 7, ref. num 502 of Watanabe et al.);
- Obtaining an encryption key and generating a shared key set including the obtained encryption keys in accordance with the determination result of the first step (see col. 6, line 57 through col. 7, line 16 of Watanabe et al.);
- Determining access authorization to an access point belonging to an LAN by a LAN authentication server which is requested to perform initial authentication by the wireless station (see fig. 7, ref. num 510 of Watanabe et al.);

- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the third step (see col. 7, lines 41-64 of Watanabe et al.);
- Determining access authorization to an access point belonging to a WAN by a WAN authentication server which is requested to perform initial authentication by the wireless station (see fig. 7, ref. num 516 of Watanabe et al.); and
- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the fifth step (see col. 7, lines 41-64 of Watanabe et al.).

Regarding claim 5, Eskicioglu as modified by Watanabe et al. teaches wherein the first step further comprises the wireless station requesting the access point to perform authentication, and the access point which is requested to perform authentication determining whether or not access authorization to the access point corresponds to a class 1, the class 1 indicating access authorization to the access point to which the wireless station is assigned (see col. 7, lines 17-40 of Watanabe et al.).

Regarding claim 6, Eskicioglu as modified by Watanabe et al. teaches wherein the third step of claim 4 further comprises:

- The LAN authentication server determining whether or not access authorization to the access point corresponds to a class 2, the class 2 indicating access

authorization to predetermined access points included in a LAN to which the wireless station is assigned;

- If a determination result indicates that the access authorization corresponds to the class 2, obtaining an encryption key of class 2, and determining whether or not the access authorization corresponds to a class 3, the class 3 indicating access authorization to all access points included in the LAN to which the wireless station is assigned; and
- If a determination result indicates that the access authorization corresponds to the class 3, obtaining an encryption key of class 3 (see fig. 4, ref. num 408A-D, 410A-B, and 412A-F of Watanabe et al.).

Regarding claim 7, Eskicioglu as modified by Watanabe et al. teaches all the limitations of claims 4 and 6, above. However, Eskicioglu as modified by Watanabe et al. does not specifically teach wherein the second step of claim 6 further comprises: allocating a null encryption key if the determination result of the first step indicates that the access authorization does not correspond to the class 2; and allocating a null encryption key if the determination result indicates that the access authorization does not correspond to the class 3.

Official Notice is taken that a null encryption key is allocated if the determining steps determines that the access authorization does not correspond to class 2 or 3.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine allocating a null encryption key based on a determination that the access authorization does not correspond to class 2 or 3, with the method of Eskicioglu/Watanabe et al. It would have been obvious for such modifications because a null encryption key ensures that access is not obtained when access authorizations do not match. When a mobile device does not have authorization for a certain class, a null encryption key will prevent further access. If the null encryption key was not allocated to the mobile device, other data would be allocated and could possibly allow authorization.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda et al. (U.S. Patent No. 6,289,102) in view of Eskicioglu (U.S. Patent Pub. No. 2002/0108040).

Regarding claim 14, Ueda et al. teaches a computer readable storage medium storing instructions which, when executed causes execution of a program implementing a structure of a wireless data packet in a wireless network that comprises a wireless station and an access point, the structure comprising:

- A header of said data packet transmitted through the wireless network (fig. 1, SECTOR HEADER FIELD);
- An encrypted data field in which data contents to be transmitted are encrypted and stored (fig. 1, USER DATA FIELD and fig. 13, section E); and

- An error correction field, which is used to correct data error (fig. 1, ECC).

Ueda et al. does not teach an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point, wherein: the access authorization information storing field comprises access authorization information being used for allocating encryption keys differentiated according to access authorization classes, and the differentiated encryption keys are provided to communicate data with corresponding access points.

Eskicioglu teaches an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point, wherein: the access authorization information storing field comprises access authorization information being used for allocating encryption keys differentiated according to access authorization classes, and the differentiated encryption keys are provided to communicate data with corresponding access points (paragraph 0038, 0047, and 0088-0094).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a field for access authorization information storing, as taught by Eskicioglu, with the medium of Ueda et al. It would have been obvious for such modifications because the access authorization field tells the device being accessed which level of access needs to take place.

Allowable Subject Matter

5. Claims 2, 9, 13, and 15 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S. HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Primary Examiner, Art Unit 2436